UNIVERSIDAD POLITÉCNICA DE

SAN LUIS POTOSÍ

CARRERA: Ingeniería en Tecnologías de la Información

MATERIA: Seguridad Informática

TRABAJO: Implementación IPsec VPN

PARCIAL 1

Aguilar Carrizales Miguel Angel / 182318

Fecha de entrega: 16 de Febrero de 2026

Introducción

IPsec (Internet Protocol Security) es un conjunto de protocolos de seguridad que opera en la capa de red del modelo OSI y permite proteger el tráfico IP mediante el uso de cifrado y mecanismos de autenticación. Al implementarse como una VPN (Virtual Private Network), IPsec crea un “túnel seguro” entre dos puntos —como sucursales de una empresa o un usuario remoto y una red corporativa— asegurando que la información transmitida no pueda ser interceptada ni modificada por terceros.

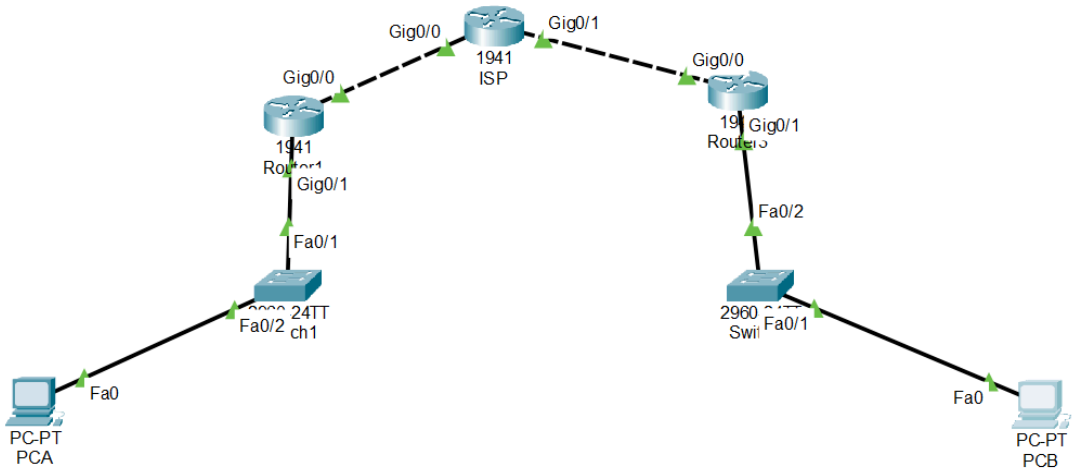
IPsec funciona mediante dos protocolos principales: el Encapsulating Security Payload (ESP), que proporciona cifrado y protección de datos, y el Authentication Header (AH), que garantiza la autenticación e integridad del tráfico. Además, utiliza el protocolo IKE (Internet Key Exchange) para negociar claves criptográficas y establecer las asociaciones de seguridad necesarias para la comunicación segura.

Gracias a su alto nivel de seguridad y compatibilidad con múltiples dispositivos de red, IPsec VPN es ampliamente utilizada en entornos empresariales para interconectar redes remotas y permitir acceso seguro a recursos internos a través de Internet.

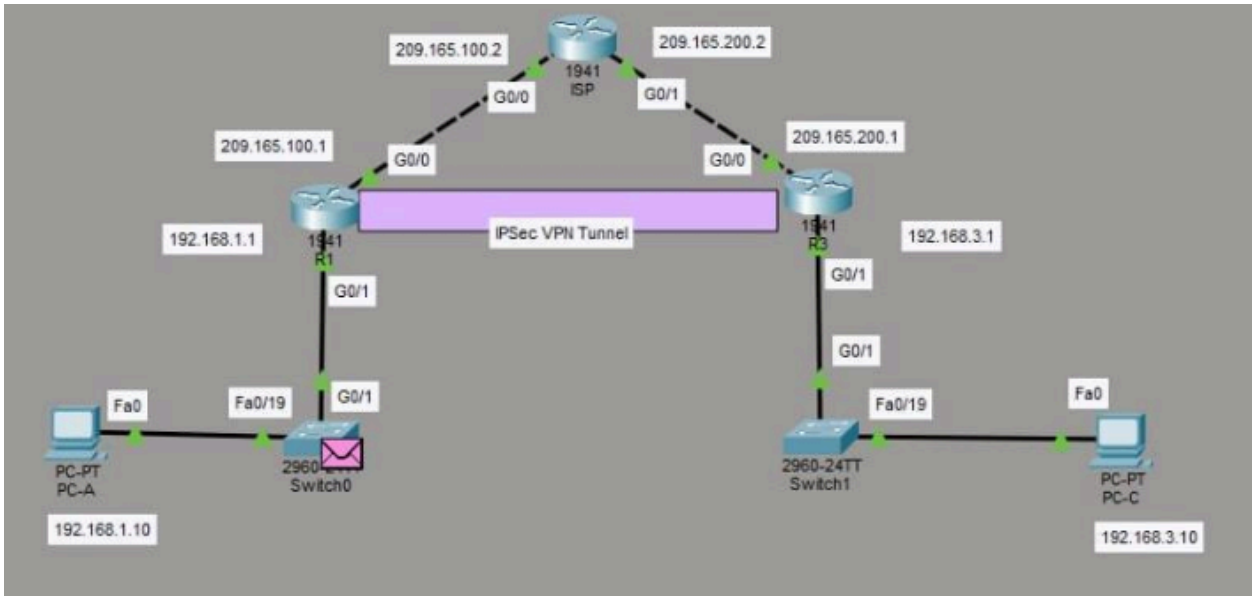
Desarrollo

1) Configuración inicial de equipo

Creamos la topología



basándonos en la topología deseada para realizar la práctica, la cual es la siguiente.



Empezamos a configurar cada router, switch y equipo final para que coincida con la topología buscada.

Router 1

```
Router>en
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 209.165.100.1 255.255.255.0
```

Le damos la dirección privada y publica correspondiente según el puerto que el toque.

```
Router#en
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
```

```
Router(config)#ip route 0.0.0.0 0.0.0.0 209.165.100.2
Router(config)#exit
Router#
```

Definimos una ruta predeterminada hacia el ISP en ambos routers.

```
Router#en
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
```

Le cambiamos el nombre para un control más simple y organizado.

Repetimos el proceso para el router 3 y el ISP.

Router 3

```
Router#conf
Configuring from terminal, memory, or network [terminal]? terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 209.165.200.1 255.255.255.0
Router(config-if)#no shutdown
```

ISP

```
Router>en
Router#configure
Configuring from terminal, memory, or network [terminal]? terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#ip address 209.165.200.2 255.255.255.0
Router(config-if)#no sh
Router(config-if)#exit
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 209.165.100.2 255.255.255.0
Router(config-if)#no shutdown
```

2) Activar paquete de seguridad (licencia de seguridad habilitada)

Usamos el comando para qué se instale la licencia.

```
Router(config)#license boot module c1900 technology-package securityk9
```

```
Router(config)#do reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
```

```
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Conf
reload


Router>enable
Router#sh run
Building configuration...

Current configuration : 736 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
 --More-- |
```

Activamos la licencia y verificamos que si se activó.

Es necesario debido a que no podemos implementar futuros pasos sin está instalación

```
!
!
license udi pid CISCO1941/K9 sn FTX15242BHG-
license boot module c1900 technology-package securityk9
!
!
```

3) implementación de ACL’s

```
R3(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#do wr
Building configuration...
[OK]
```

```
R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#do wr
```

Se implementan las access lists en los dos routers para qué deje entrar paquetes del otro dispositivo final. Específicamente del ip privado del otro routes.

4) Phase 01: ISAKMP policy

```
Router(config)#hostname R1
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
```

Se establece la política número 10 de isakmp, se utiliza la encriptación de 256 bits, se usa pre-share para la autenticación por clave pre compartida y usamos el grupo 5 para el intercambio de claves.

5) Phase 02 IPsec transform set.

```
R1(config)#crypto isakmp key secretkey address 209.165.200.1
R1(config)#crypto ipsec transform-set R1-R3 esp-aes 256 esp-sha-hmac
```

Establecemos clave compartida con R3.

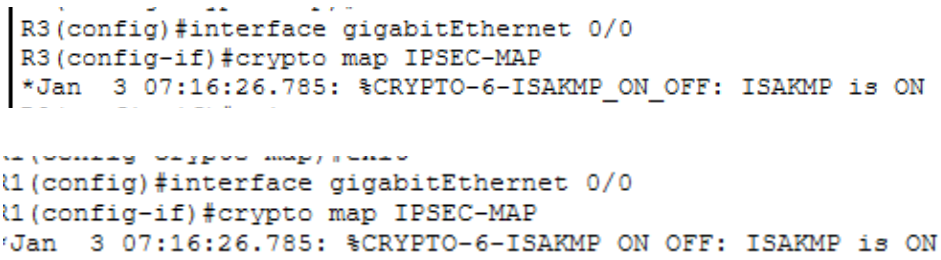
En la siguiente línea establecemos el conjunto de transformación con cifrado aes y autenticación sha

6)Crear el mapa criptográfico

```
R3(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)#set peer 209.165.100.1
R3(config-crypto-map)#set pfs group 5
% Ambiguous command: "set pfs group 5"
R3(config-crypto-map)#set security-association lifetime seconds 86400
R3(config-crypto-map)#set transform-set R3-R1
R3(config-crypto-map)#match address 100
R3(config-crypto-map)#exit
```

Creamos el mapa criptográfico con secuencia 10, después definimos la ip pública del peer remoto que es el router 3, se establece el tiempo de la asociación a 24 horas, finalmente creamos el túnel y definimos le match address en 100 para qué coincida con la ACL qué creamos.

7)Aplicar el mapa criptográfico



Entramos a las interfaces para aplicar el mapa y asegurarnos que están encendidos.

Conclusión

Los pasos hasta los que se llegaron son claves para hacer que la simulación pueda funcionar y estemos cerca de la configuración de una IPsec VPN. La práctica en Packet Tracer permitió validar de manera práctica la configuración de IPsec VPN, reforzando los conceptos teóricos y demostrando cómo esta tecnología protege la comunicación entre sedes empresariales en un entorno simulado.